ABSTRACT

A trusted computing platform includes one or more first logically protected computer environments (or "compartments") associated with initialisation of the system, and one or more second logically protected computing environments (or "compartments"). The one or each second compartment is associated with at least one service or process supported by the said system. The trusted computing platform is loaded with a predetermined security policy including one or more security rules for controlling the operation of each of the compartments such that the security rules relating to the one or each first compartment is loaded onto the trusted computing platform when the system is initialized. The one or more security rules relating to the one or at least one of the second compartments are only loaded onto the trusted computing platform if one or more services or processes associated therewith are enabled.